Jülich Supercomputing Centre

Ein IPS für JuNet

Juli 2015

Egon Grünter, Markus Meier, Ralph Niederberger

Interner Bericht · FZJ-JSC-IB-2015-02

JÜLICH
FORSCHUNGSZENTRUM

FORSCHUNGSZENTRUM JÜLICH GmbH
Jülich Supercomputing Centre
D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

Ein IPS für JuNet

Egon Grünter, Markus Meier, Ralph Niederberger

FZJ-JSC-IB-2015-02

November 2014

(letzte Änderung: 24.07.2015)

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einleitung

Informationen, Daten und ein freier Zugang zu Kommunikationsnetzen sind ein wertvolles Gut, besonders in Wissenschaft und Forschung. Der Schutz dieser Ressourcen sowie der dazugehörenden Einrichtungen der Informationstechnik (IT) ist Gegenstand und Aufgabe der IT-Sicherheit. Im Rahmen des IT-Sicherheitskonzeptes des Forschungszentrums Jülich stellt das JSC zentrale Dienste und Ressourcen für die operationale IT-Sicherheit zur Verfügung.

Zu den Aufgaben des JSC im Rahmen der operationellen Sicherheit zählt vor allem auch der Betrieb von zentralen Sicherheitskomponenten wie Firewalls und Intrusion Detection/Prevention Systeme (IDS) (vgl. Richtlinie Nr. 2/2012 IT-Sicherheitsrichtlinie des Forschungszentrums Jülich - §8 Aufgaben des Jülich Supercomputing Centre (JSC) - Unterpunkt 3) [JSC-RI-2-2012]. Eine ausführliche Beschreibung von Intrusion Detection Systemen bietet die BSI Studie „Einführung von Intrusion-Detection-Systemen“ aus dem Jahre 2002 [BSI-IDS-Grundlagen]. Wenn auch bereits 10 Jahre alt, beschreibt die Studie ausführlich die diversen Problemstellungen, Einsatzszenarien, Risiken und Chancen die sich durch den Betrieb von IDS-Systemen ergeben.

Bisher wurden am Zugang des Forschungszentrums lediglich zentrale Firewall-Systeme zum INTERNET hin betrieben sowie durch JSC selbst erstellte Intrusion Detection Mechanismen verwendet. Auf den Server-Systemen und Arbeitsplatzrechnern wird zusätzlich verlangt host-basierte Firewall-Systeme (Software-Lösungen) zu installieren. Diese Maßnahmen etablieren ein zweistufiges Sicherheitskonzept, das sich in der heterogenen IT-Landschaft des JuNet bewährt hat.

Im Bereich der Intrusion Detection/Prevention wurde bisher empfohlen auf den lokalen Systemen Log-Dateien zu erstellen und diese kontinuierlich auf Unregelmäßigkeiten zu überprüfen. Ferner helfen sogenannte „System Integrity Verifiers“ durch Überprüfung von Prüfsummen, unberechtigte Veränderungen am System zu identifizieren.

Auf zentraler Ebene konnte bisher keine ausführliche Intrusion Detection/Prevention realisiert werden, da die Systeme den Anforderungen in einem wissenschaftlich-technischen Umfeld mit seinen vielfältigen, heterogenen und häufigen Änderungen unterworfenen Kommunikationsbeziehungen nicht genügten. Eine Angriffserkennung erfolgte bisher auf Basis von Eigenentwicklungen des JSC, die besonders häufige Angriffe erkennen und teilweise proaktiv verhindern. Allerdings werden die Angriffe immer weniger offensichtlich und zunehmend komplexer, so dass Eigenentwicklungen auf Basis statistischer Maßzahlen wenig erfolgversprechend sind.

Lt. Bericht des Bundeskriminalamtes zu „Cybercrime – Bundeslagebild 2011“ entwickelt sich das „Phänomen Cybercrime“ weiterhin dynamisch [CYBERCRIME]. Sicherheitsmaßnahmen werden sehr schnell durch geeignete Schadsoftware überwunden. Diesem Umstand ist verstärkt Rechnung zu tragen, indem Attacken früher erkannt bzw. gänzlich verhindert werden, um Schäden aller Art (finanziell, Aufgabenerfüllung, juristisch, Reputation) vom Forschungszentrums abzuhalten.

Das JSC führt seit Jahren Forschungs- und Entwicklungsarbeiten zu IT-Sicherheitsthemen durch. So arbeitet die Abteilung Kommunikationssysteme des JSC in nationalen und internationalen Projekten an der Weiterentwicklung von IT-Sicherheitslösungen mit. Sowohl das Beta-Testing von Hochgeschwindigkeits-Firewalls, Intrusion Detection/Prevention und Security Monitoring als auch die Mitarbeit in internationalen Standardisierungsbemühungen im Bereich der dynamischen Konfiguration von Firewalls bieten frühen Einblick in neue Entwicklungen. Das durch diese Aktivitäten erworbene und gestärkte Know-how ermöglicht dem JSC, in dem komplexen Umfeld eines vielfältig vernetzten Forschungs- und Supercomputing-Zentrums IT-Sicherheitslösungen auf dem jeweiligen Stand der Technik zu implementieren und zu betreiben.

Im Rahmen dieser Arbeiten wurden Tests diverser IDS/IPS-Systeme durchgeführt. Diese zeigten auf, dass kontinuierlich neue Angriffe auf Rechnerressourcen des Forschungszentrums Jülich gefahren werden. Die von den Angreifern verwendeten Tools werden dabei immer komplexer und ausgefeilter, sodass das Risiko eines Sicherheitsvorfalles mit größerem Schaden zunimmt. Diesem Umstand haben auch die Entwickler von IDS/IPS-Systemen Rechnung getragen und ihre Systeme verfeinert, sowie die verwendeten Tools immer leistungsfähiger und performanter gemacht. Wie Tests im Jahr 2012 gezeigt haben, haben kommerzielle IDS/IPS-Systeme inzwischen eine Qualität erreicht, die auch einen effektiven Einsatz in einem so komplexen Umfeld wie dem Forschungszentrum ermöglicht. Mit dem Betrieb eines kommerziellen Angriffserkennungssystems würde daher ein zusätzliches Maß an Sicherheit gewonnen.

Mit der Beschaffung eines solchen Systems nimmt das JSC seine in der IT-Sicherheitsrichtlinie der Forschungszentrum Jülich GmbH (IR 119-1), beschriebenen Aufgaben im IT-Sicherheitsmanagement des Forschungszentrum Jülich wahr.

In diesem Bericht werden die Anforderungen, die Tests und deren Ergebnisse beschrieben. Abschließend wird ein mögliches Einsatzszenario eines IDS/IPS-Systems vorgestellt. Mit einem Ausblick auf zukünftig mögliche Erweiterungen wird das vorgestellte Konzept abgerundet.

2. Anforderungen

Vor der Auswahl geeigneter Testsysteme wurden Anforderungen an ein Intrusion Prevention System spezifiziert, die letztlich als Bewertungsgrundlage der Testergebnisse dienen. Daher wird zunächst die Funktionsweise eines Angriffserkennungssystems erläutert, so dass die gestellten Anforderungen speziell auf das Campusnetzwerk JuNet zugeschnitten werden können.

2.1 Erkennung von Angriffen

Im Allgemeinen kann ein Intrusion Detection/Prevention System mit einem Virenscanner verglichen werden. Ein Virenscanner auf einem Client-PC analysiert im Hintergrund Dateien und vergleicht diese mit vorhandenen Mustern, den sog. Signaturen, und möglichen Änderungen. Darüber hinaus verfügen aktuelle Virenscanner über heuristische Verfahren, die als Ergänzung zu den bereits bekannten Mustern zu sehen sind und den Virenscannern damit die Möglichkeit bieten, unbekannte Schadsoftware zu erkennen.

Beide Analyseverfahren sind auf IPS-Systeme übertragbar. Bekannte Angriffe werden über Signaturen erkannt. Als Beispiel dient hier die aktuelle Shell-Shock-Schwachstelle (CVE-2014-6271), die mit der folgenden Befehlssequenz auf der Kommandozeile einer Linux-Konsole getestet werden konnte.

```
env x='() { :;}; echo shellshockverwundbar' bash -c ""
```

Eine mögliche Signatur zur Angriffserkennung könnte z.B. innerhalb eines http-Streams die Zeichenkette `() {` darstellen. Erkennt das System dieses Muster, könnte der Hinweis auf einen möglichen Angriff gegeben sein, und nötige Gegenmaßnahmen müssten dann getroffen werden.

Unbekannte Angriffe zeichnen sich also in diesem Kontext dadurch aus, dass keine Signatur existiert. Zur Angriffserkennung können dann also nur statistische Maßzahlen, sog. Profile, herangezogen werden. Das System erstellt dazu eine Basis (Baseline), die als Normalverhalten eines Rechners oder eines Teils des Netzwerkes angenommen wird. Abweichungen von diesem Profil sind dann Hinweise auf einen möglichen Vorfall.

Die folgende Abbildung 1 zeigt in einem Diagramm die Baseline und das Verhalten der zurückliegenden Woche bzgl. eines Clients-PCs und der Anzahl http-Verbindungen zu externen Servern. Es ist deutlich zu sehen, dass am Donnerstag ein anomales Verhalten des Clients vorliegt, da die Anzahl der http-Verbindungen signifikant abweicht (ansteigt). Damit ist ein möglicher Sicherheitsvorfall erkannt worden. Diese Erkennungsart wird auch als Anomalieerkennung bezeichnet.

Die beiden hier gezeigten Beispiele verdeutlichen nicht nur die Funktionweise der Angriffserkennung, sondern auch deren mögliche Nachteile. In beiden Fällen könnte der

Alarm ein Fehlalarm („False positive“) sein. Betrachten wir z.B. eine http-Stream, der einen C-Programmquelltext überträgt und die folgende Funktionsdefinition enthält:

```
int printMeldung() {…
```

In diesem Fall würde die oben angegebene Signatur ebenfalls einen Alarm auslösen.

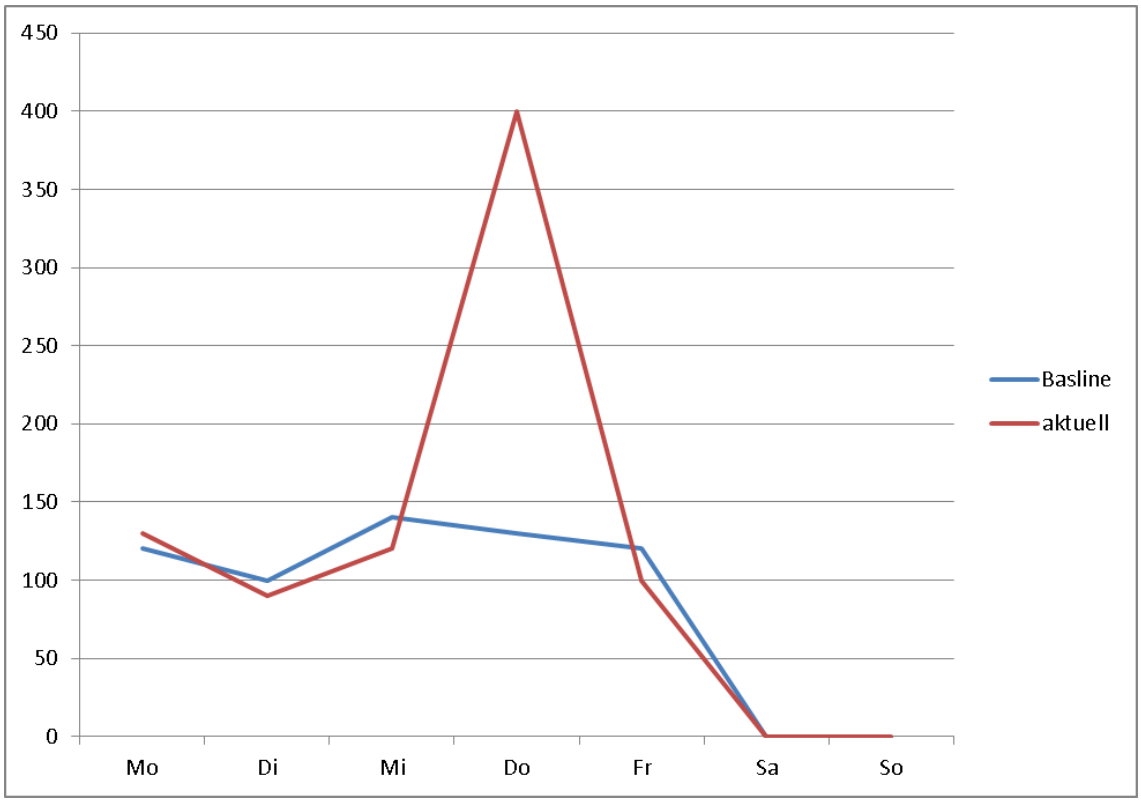

Abbildung 1: Mögliches Profil eines Client-PCs

Im Beispiel der Anomalieerkennung könnte es sich in diesem Fall um einen Client-PC handeln, der automatisiert eine Vielzahl von Messergebnisdateien von einem externen Server lädt.

Im Betrieb eines IDS/IPS-Systems ist die Unterscheidung zwischen Fehlalarmen und korrekten Alarmen eine wesentliche Aufgabe des Administrators. Durch verbesserte und detaillierte Signaturen, sowie Baselines über längere Zeiträume hinweg, kann die Anzahl der Fehlalarme minimiert werden. Regelmäßiges Fein-Tuning durch den Administrator kann die Erkennungsrate also wesentlich verbessern.

Wie in der Einleitung bereits erwähnt, haben Tests im Jahre 2012 gezeigt, dass kommerzielle IDS/IPS-Systeme in der heterogenen IT-Landschaft des Forschungszentrums durchaus effektiv betrieben werden können, d.h. die Fehlalarmrate der damaligen Tests hatte sich gegenüber vorhergehenden Tests so entschieden verbessert, dass eine weitere Minimierung durch Automatismen fast nicht weiter möglich scheint. Lediglich durch manuelle Anpassungen sind weitere Verbesserungen zu erzielen.

Die beiden beschriebenen Angriffserkennungsverfahren können also unterteilt werden in die Erkennung bekannter Angriffe (signatur-basierte Erkennung) und unbekannter Angriffe (anomalie-basierte Erkennung). Daher ist es eine Anforderung an das auszuwählende System beide Arten von Angriffen zu erkennen, wobei ein Schwerpunkt auf der signaturbasierten Erkennung liegt.

2.2 Verschlüsselte Datenübertragungen

Aufgrund der vorhergehenden Betrachtungen zur Angriffserkennung wird deutlich, dass signaturbasierte IPS-Systeme nur dann alarmieren, wenn die analysierte Kommunikation unverschlüsselt erfolgte. Bekannte Beispiele für unverschlüsselte Anwendungsprotokolle sind http, telnet, imap, pop und smtp. Bei diesen Protokollen können alle bekannten Angriffe von Wörterbuchangriffen bis hin zu Buffer-Overflows erkannt werden.

Diese Möglichkeit ist so nicht mehr gegeben, wenn die Kommunikation kryptographisch gesichert erfolgt, z.B. mit OpenSSL. https, imaps, pops sind die bekanntesten Vertreter dieser Protokolle. Für den Zugang zu entfernten Rechnern ist SSH die bekannteste Variante. Der Klartext der Nutzdatenübertragung ist nur auf den an der Kommunikation beteiligten Systemen verfügbar.

Für die Analyse des Klartextes müsste ein IDS/IPS-System derart in die Kommunikation eingreifen, dass es als Man in the middle zwischen Client und Server sitzt, und zu jedem Partner eine eigens verschlüsselte Verbindung unterhält (vgl. Abbildung 2).

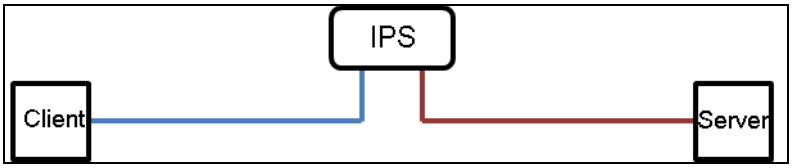

Abbildung 2: IPS als Man in the middle

Diese Technologie ist in vielen aktuellen signaturbasiereten IDS/IPS-Systemen enthalten. Sie unterbricht die zur Verschlüsselung notwendigen Vertrauensstellungen bei X.509-Zertifikaten, in dem das IDS/IPS-System als Certificate Authority (CA) arbeitet und on-demand Zertifikate für den angesprochenen Server erstellt. Bei der Entschlüsselung von Secure Shell arbeitet das System ähnlich, indem es sich immer mit dem gleichen Host-Key-Pair in die Kommunikation einschleift.

Für JuNet-Clients ist diese Art der Entschlüsselung momentan nicht vorgesehen. Ein Grund für diese Entscheidung stellt dabei die lt. Gesamtrahmenbetriebsvereinbarung Informations- und Kommunikationssysteme im geringen Umfang erlaubte private Nutzung der IuK-Systeme im JuNet dar. Darüber hinaus sind technische und Policy-bezogene Probleme zu erwarten, wenn Server-Zertifikate durch die einer anderen CA ersetzt werden.

Angriffe über verschlüsselte Anwendungsprotokolle fallen somit unter dem Gesichtspunkt der zentralen Angriffserkennung in die Kategorie der unbekannten

Angriffe, die über anomalie-basierte Analyse erkannt werden sollen. Es wird daher nicht gefordert, dass das zu beschaffende IDS/IPS Verschlüsselung aufbrechen kann.

2.3 Topologie

JuNet, das schnelle Rechnernetz des Forschungszentrums Jülich ist seit Anfang 1989 in Betrieb und unterstützt das Kommunikationsprotokoll INTERNET (TCP/IP). Das Netz ist als **"offenes Netz"** konzipiert, d.h. jeder Mitarbeiter des Forschungszentrums hat die Möglichkeit, IT-Systeme für Belange seiner dienstlichen Tätigkeiten an dieses Netz anzuschließen und die bereitgestellten Ressourcen zu nutzen.

JuNet besteht physikalisch aus einer hierarchisch organisierten Struktur von Layer2/3 Switches, über welche die an JuNet teilnehmenden Geräte untereinander und mit dem weltweiten Internet verbunden werden.

Alternativ zum Festnetzanschluss steht in großen Teilen des Forschungszentrums eine WLAN-Infrastruktur (W-JuNet) zur Verfügung, welche kontinuierlich erweitert wird. Über diese kann ein Anschluss an ein Mitarbeiter-WLAN oder Gäste-WLAN realisiert werden. Das Mitarbeiter-WLAN ermöglicht den Teilnehmern im Gegensatz zum Gäste-WLAN direkten Zugriff auf das interne Netz, wie man es im kabelgebundenen Netz gewohnt ist.

Um auch Übergänge zwischen JuNet und den externen Netzen (**Internet**) zu ermöglichen, betreibt das JSC mehrere Router zur Anbindung an das Wissenschaftsnetz (X-WiN) des DFN. Die Übergänge sind durch Firewalls gesichert. Damit ergibt sich für JuNet die folgende Topologie.

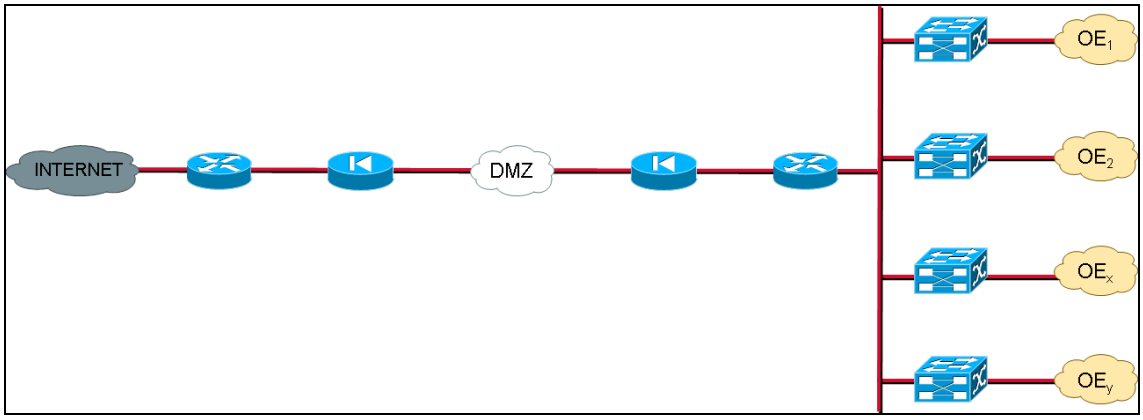

Abbildung 3: Schematische Darstellung des JuNet

Während die Firewalls die Übergänge zwischen unterschiedlichen Sicherheitszonen realisieren, sollte eine IDS/IPS ein möglichst großes Analysevolumen abdecken und so den Datenverkehr innerhalb der Sicherheitszonen auf mögliche Angriffe hin untersuchen.

Damit ist die dritte Anforderung an das IDS/IPS-System spezifiziert: Das System muss möglichst verteilt installierbar sein und mit unterschiedlichen Konfigurationen entsprechend der Einsatzumgebung arbeiten.

2.4 Internet-Protokolle

Im Rahmen von JuNet wird ausschließlich die TCP/IP-Protokoll-Familie unterstützt, das bedeutet als Internet-Protokoll werden die Versionen 4 und 6 (IPv4, IPv6) genutzt. Ein zu installierendes Angriffserkennungssystem muss deswegen in der Lage sein, sowohl Angriffe über IPv4 als auch Angriffe über IPv6 zu erkennen. Die folgende Abbildung verdeutlicht beispielhaft Unterschiede und Gemeinsamkeiten der Angriffe.

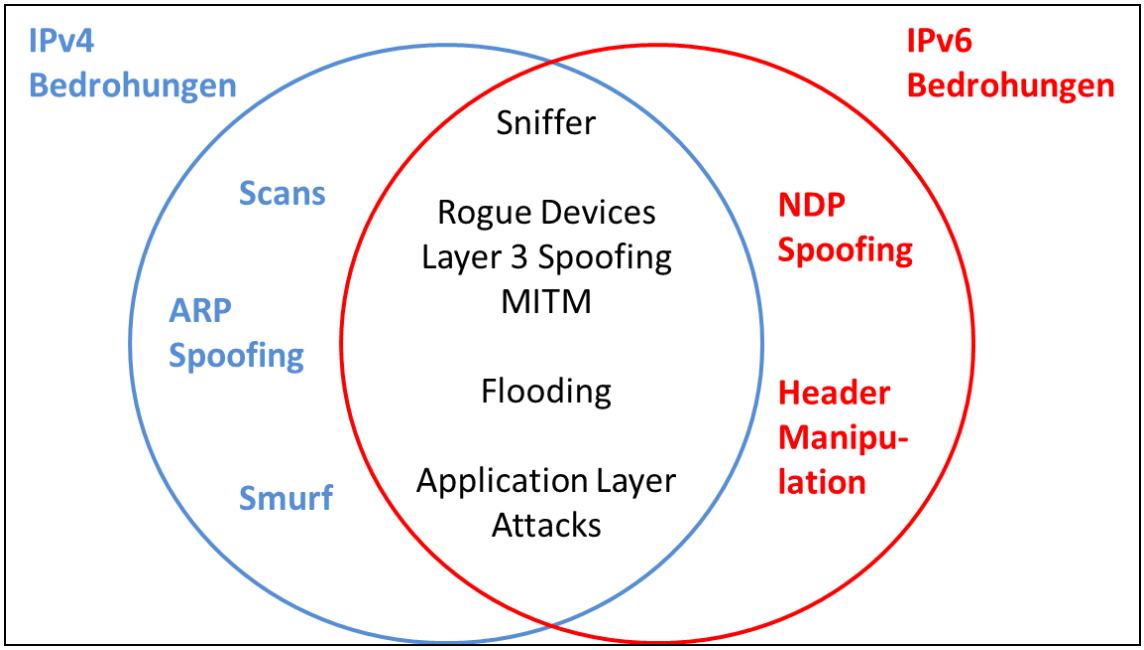

Abbildung 4: Angriffe IPv4 und IPv6

Aus der vorhergehenden
Abbildung 4 geht hervor, dass die Phasen eines geplanten Angriffs sowohl über IPv4 als auch über IPv6 erfolgen können. Die Erkundung oder auch das Rastern des Netzwerks (Scanning) wird sicherlich über IPv4 erfolgen, wohingegen die Phase eigentlichen Zugriffs und dessen Verwaltung über IPv6 durchgeführt werden können. Optimal wäre ein Intrusion Detection/Prevention System, dessen Alarmierung diese scheinbar unabhängigen Angriffe als zusammenhängend korreliert.

Damit sind auch die Anforderungen an die Analyse der Protokollfamilien formuliert.

2.5 Syslog & API

Ein wesentlicher Schwerpunkt der im folgenden Kapitel beschriebenen Tests soll auf der Integration des IDS/IPS-Systems in die bestehende Produktionsumgebung des vom JSC betriebenen Campusnetzwerks JuNet liegen.

Dazu ist es notwendig, dass Alarmierungen des Systems per Syslog an das Splunk>-Cluster des JSC geschickt werden können. Das Splunk>-Cluster des JSC sammelt Syslog unterschiedlicher Quellen, stellt mit seiner komfortablen Suchsprache eine Echtzeitalarmierung bereit und stellt mit der vorhanden REST-API einen wesentlichen Bestandteil des Security Information and Event Management (SIEM) „JuSIEM“ des JSC dar.

Gleichzeitig ist es wichtig, dass ein IDS/IPS-System Informationen aus weiteren SIEM-Komponenten erhalten kann. Dazu zählen neben kurzfristigen Reaktionen auf die jeweils aktuelle Bedrohungslage in Form von Konfigurationsänderungen auch Informationen von Schwachstellen- und Patch-Management-Systemen, auf deren Basis die Fehlalarmrate minimiert werden kann. Das Angriffserkennungssystem sollte über ein Application Programming Interface (API) verfügen, so dass Anpassungen und (halb-)automatisierte Reaktionen zur Isolation von bedrohten Systemen durchgeführt werden können.

2.6 Management

Die tägliche Administration und Konfiguration ist neben der Prüfung der Alarme eine der Hauptaufgaben der Administratoren des IDS/IPS-Systems. Deswegen werden auch in diesem Bereich Anforderungen an das System gestellt.

Im Zuge fortschreitender Nutzung des Internet Protocols Version 6 (IPv6) ist es zwingend notwendig, dass das IPS-System über IPv6 administriert werden kann. Das bedeutet, dass das System alle verpflichtenden IPv6-Standards unterstützt und so konfiguriert werden kann, dass die Anforderungen des JuNet-Managements erfüllt werden. Die Web- oder Konsolenschnittstelle zur Konfiguration des Systems muss also über IPv6 erreichbar sein.

Neben den administrativen Zugängen sollte ebenfalls die Möglichkeit bestehen, das System in ein bestehendes Managementsystem zu integrieren. Das bedeutet, dass entweder über graphische Benutzeroberflächen (GUIs) oder per existierender oder noch zu entwickelnder Scripte Administrationsaufgaben erledigt werden können.

Neben der Administration muss aber auch die Überwachung im Hinblick auf die Verfügbarkeit gegeben sein, das bedeutet, dass Standardverfahren und –protokolle wie das Simple Networks Management Protocol (SNMP) oder agentenbasiertes Monitoring möglich sein müssen.

3. Tests

In diesem Kapitel werden die Testkandidaten, die Tests und ihre Randbedingungen näher erläutert. Im darauf folgenden Kapitel werden die Ergebnisse detailiert analysiert.

3.1 Auswahl der Testkandidaten

Im Rahmen des IDS/IPS-Projektes wurde vereinbart, dass zu Beginn eine mindestens drei monatige Testphase inkl. Marktanalyse durchgeführt wird.

Zur Marktanalyse wurden zunächst Testberichte von Gartner[1] und den NSS Labs[2] als Informationsquelle genutzt. Während dieser Phase zeigte sich, dass eine Unterscheidung im klassischen Sinn zwischen Firewall und Intrusion Detection/Prevention System so nicht mehr gegeben ist. Stattdessen werden derartige Syteme häufig als Unified Threat Management Systems (UTM) bezeichnet.

Im Allgemeinen versteht man unter einem UTM eine Security-Lösung, die eine Vielzahl von Services bereitstellt. Dazu zählen Firewall-, IDS/IPS-, VPN-, URL-Filter-, DLP-, Antivirus-Lösungen und andere. Next Generation Firewalls und Next Generation IPSs, deren Entscheidungskriterien nicht mehr nur auf IP-Adressen und TCP- oder UDP-Ports fußen, sondern auf Informationen wie z.B. genutzte Applikation, Benutzername oder Patch-Level des Systems, sind Unterarten der UTMs.

Während der Marktanalyse wurden UTMs, Next Generation Firewalls und Next Generation IPSs gleichermaßen berücksichtigt. In den Gartner Testberichten von Februar 2013 und April 2014 für Enterprise Firewalls, inklusive Next Generation Firewalls, liegt Palo Alto im Magic Quadrant im Bereich der „Leaders“ und „Visionaries“ und demzufolge im oberen Preissegment. Das JSC hat aufgrund der schon seit langem exponierten Stellung bereits frühzeitig, seit ca. 2008, immer wieder Teststellungen mit Palo Alto durchgeführt und verschiedene Geräte getestet. Auch aufgrund dieser Erfahrungen wurde Palo Alto Networks in die Liste der Testkandidaten aufgenommen.

Im Magic Quadrant 2013 und 2014 für UTMs ist Fortinet als führender Hersteller vertreten (vgl. Abb. 6). Ebenfalls sahen die Tester der NSS Labs im Jahre 2013 Fortinet unter den Topherstellern für Next Generation Firewalls und Next Generation IPS (vgl. Abb. 7). Im Rahmen der Marktanalyse wurden auch Security Veranstaltungen besucht, bei denen Kontakt zu Fortinet hergestellt und erste Eindrücke gewonnen werden konnten. Aufgrund dieser Eindrücke und gewissen Ähnlichkeiten in der Bedienoberfläche zu den Palo Alto Geräten, wurde Fortinet als weiterer Testkandidat ausgewählt.

[1] http://www.gartner.com/technology/about.jsp
[2] https://www.nsslabs.com/company/about-nss

Abbildung 5: Gartner Magic Quadrant Next Generation Firewalls 2014[3]

Figure 1. Magic Quadrant for Unified Threat Management

Source: Gartner (August 2014)

Abbildung 6: Gartner Magic Quadrant UTM 2014[4]

[3] http://www.gartner.com/technology/reprints.do?id=1-1T607HL&ct=140415&st=sb
[4] http://www.fortinet.com/resource_center/analyst_reports/gartner-mq-utm-2014.html

SNORT wurde schon in früheren Tests analysiert und zeigte in der Bedienbarkeit starke Schwächen. Aufgrund der Vielzahl von Signaturen und Regeln ist die Konfiguration zur Anpassung an die Umgebung des Campus Netzwerkes JuNet sehr zeitintensiv. Ausserdem werden weitere Software-Komponenten für die Visualisierung der Alarmierungen und der Bearbeitung eben dieser benötigt. Daher wurde auf den Test der Opensource Lösung verzichtet und stattdessen SourceFire als Testkandidat mit berücksichtigt.

Zusätzlich wurde das Produkt StealthWatch der Firma Lancope in den Kreis der Testkandidaten aufgenommen. Das Produkt wurde auf diversen Security-Veranstaltungen vorgestellt und basiert auf der Auswertung von NetFlow-Information. NetFlow-Informationen werden im Detail im nächsten Kapitel beschrieben. Ein Grund für die Auswahl als Testkandidat war, dass StealthWatch bereits vorhandene Informationen der Netzwerk-Infrastruktur unter Sicherheitsaspekten auswerten und aufbereiten kann.

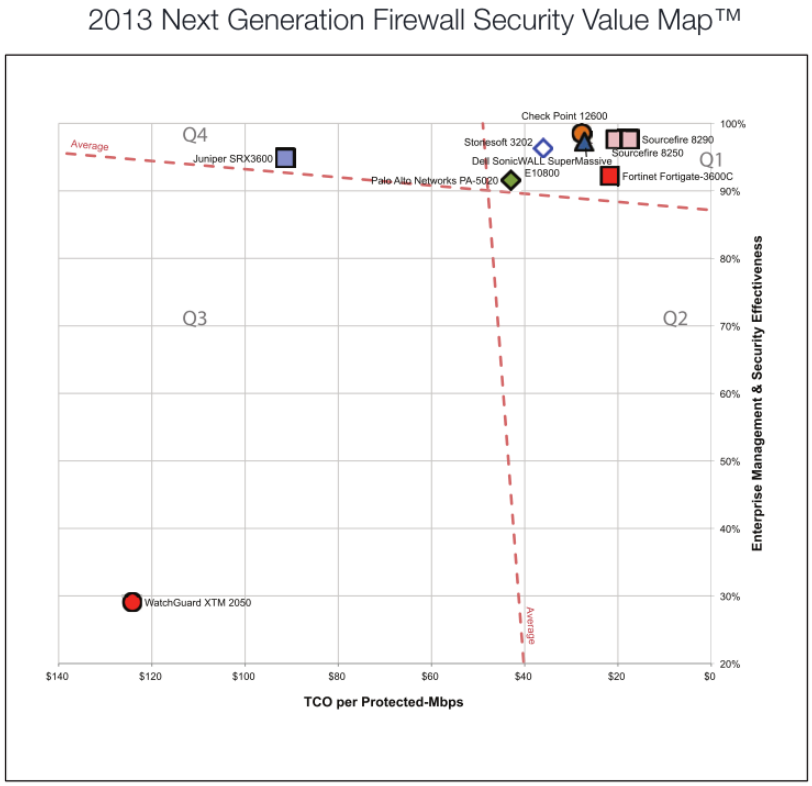

Abbildung 7: NSS Labs Test Fortinet

Abbildung 8: Gartner Magic Quadrant NextGen IPS 2013[5]

3.2 Testumgebung

Als Testumgebung wurde das Wireless LAN des Junet (W-JuNet) ausgesucht. Dieses Netz bietet Gästen der Forschungszentrumsmitarbeiter die notwendige Konnektivität. Die Vielzahl der Systeme und insbesondere auch die Tatsache, dass deren Administration nicht immer auf den Standards des Forschungszentrums basiert machen das W-LAN zu einer exponierten Testumgebung für Angriffserkennungssysteme, da die Wahrscheinlichkeit für die Anzeige von Alarmen deutlich höher liegt im Vergleich zum internen Netzwerk. Daher wurden die Geräte von Palo Alto, Fortinet und Sourcefire als transparente Devices konfiguriert, so dass jeder Verkehr aus und in das W-LAN vom Testsystem analysiert werden konnte (vgl. Abbildung 9).

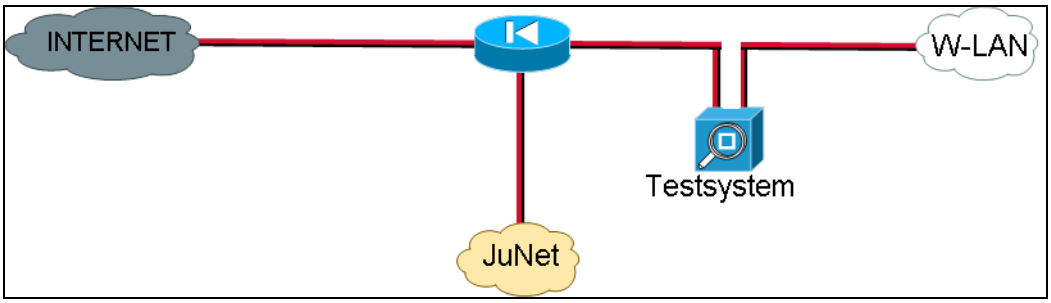

Abbildung 9: Testumgebung

[5] http://www.gartner.com/technology/reprints.do?id=1-1OR69EO&ct=131231&st=sb

Die In- und Außerbetriebnahme der Testsysteme läuft, entgegen des Eindrucks der schematischen Skizze, für die Benutzer nahezu transparent und unterbrechungsfrei, da die Verkehrsführung auf Basis des IEEE[6] 802.1q Standards[7] erfolgt.

Für das Produkt der Firma Lancope stellt das gesamte JuNet die Testumgebung dar. Hier wurden Netflow-Informationen der bestehenden Netzwerkinfrastruktur (Switches, Router, Firewalls) analysiert. Dazu wurden die Netzwerkgeräte so konfiguriert, dass sie die gewünschten Informationen an einen sog. Netflow-Collector senden. Der Netflow-Collector aggregiert und korreliert die gesendeten Daten.

3.3 Randbedingungen

Während der Marktanalyse und der Planung der Testphase wurde intensiv mit den Herstellern über Teststellungen und Zeiträume verhandelt. Die größte Schwierigkeit lag darin, dass alle Hersteller – mit Ausnahme von Lancope – ihre Testsysteme nur in begrenztem Umfang zur Verfügung stellten. Der übliche Zeitrahmen für Teststellungen betrug 30 Tage. Allerdings waren die Testsysteme zu jeweils unterschiedlichen Zeitpunkten verfügbar, so dass parallele Tests mit allen Geräten nicht möglich waren.

Aufgrund dieser Tatsache kann auch die Erkennungsrate von Angriffen auf Basis der durchgeführten Tests nicht ausreichend bewertet werden, da die Umgebung des Gästenetzes sehr dynamisch ist und sich täglich verändert. Da aber Palo Alto, Fortinet und SourceFire in den Gartner-Test sehr gut abgeschnitten haben, sind die Grundfunktionalitäten aus Sicht des Testteams bereits ausreichend gut getestet worden.

Eine Verzögerung im Ablaufplan des Projektes entstand dadurch, dass SourceFire Anfang 2014 von der Firma Cisco Systems akquiriert wurde. Erst nachdem Verwaltungsstrukturen beider Firmen so weit zusammengewachsen waren, dass Personal zur Testbetreuung und Testgeräte bereit standen, konnte mit den entsprechenden Tests begonnen werden. Ende Mai startete die Testphase mit SourceFire, nachdem Testphasen anderer Geräte bereits abgeschlossen waren.

Dennoch konnten in den Tests ausreichend Erfahrungen zur Bedienung und Verwaltung gewonnen werden, und die in Kapitel 2 gestellten Anforderungen mit der Funktionalität verglichen werden.

[6] Institute of Electrical and Electronics Engineers
[7] http://www.microhowto.info/tutorials/802.1q.html

4. Testergebnisse

4.1 Palo Alto Networks

Palo Alto Networks Inc. wurde im Jahr 2005 gegründet. Chief Technology Officer ist der Firmengründer Nir Zuk, der zuvor bei Check Point, NetScreen Technologies und Juniper Networks Firewalls und IPS-Systeme entwickelt hat. Im Jahr 2007 erschien die erste Firewall des Unternehmens. Der Börsengang erfolgte im Jahr 2012.

Als Testgerät wurde eine PA-5020[8] bereitgestellt. Sie bietet 5 Gb/s Firewall-Durchsatz, 2 Gb/s Intrusion-Prevention-Durchsatz und ansonsten alle Funktionalitäten größerer Modelle, die von den Performance-Daten her eher für einen Einsatz im JuNet geeignet wären.

Das System wird über eine Web-Schnittstelle administriert und konfiguriert. Zentraler Bestandteil ist das Application Command Center (ACC). Hier werden in Diagrammen Informationen dargestellt, die aus der Analyse des weitergeleiteten Netzwerkverkehrs stammen.

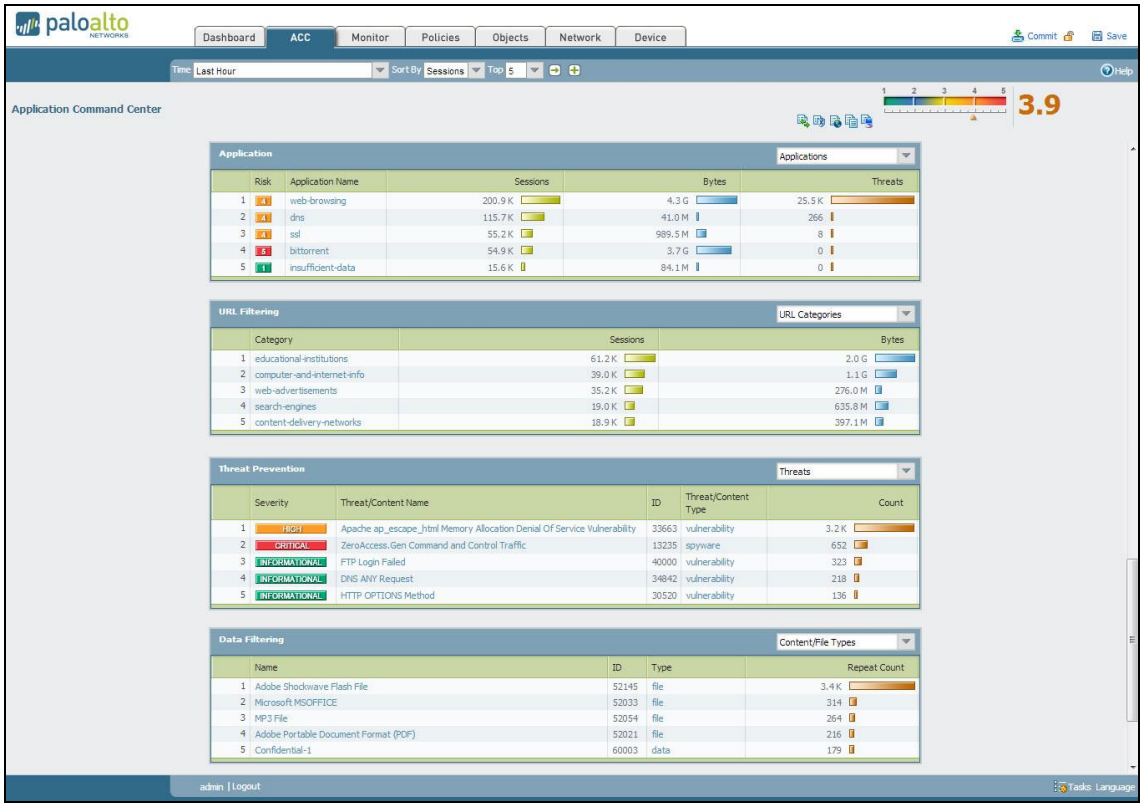

Abbildung 10: Application Command Center

Abbildung 10 zeigt einen Screenshot eines ACC. Im oberen Teil werden die Top 5 der erkannten Applikationen dargestellt. Die Kategorie „insufficient-data“ entsteht, wenn

[8] https://www.paloaltonetworks.de/products/platforms/firewalls/pa-5000/overview.html

das Gerät erst kürzlich in den laufenden Betrieb integriert wurde und noch nicht alle notwendigen Informationen, z.B. einer TCP-Session, zur Verfügung stehen.

Im zweiten Block werden die Top 5 URL-Kategorien der letzten Stunde aufgelistet. Diese Informationen werden aus der Analyse der http-Streams gewonnen. Die aufgerufenen URLs werden dann in vom Hersteller vorgegebene Kategorien eingeordnet.

Im dritten Block werden Informationen über mögliche Gefährdungen, sog. Threats, angezeigt. Die erste Zeile weist auf eine mögliche Bedrohung durch eine Apache-Webserver-Schnittstelle hin, deren potenzielle Ausnutzung vom System erkannt wurde. Dabei ist in dieser Anzeige allerdings nicht direkt erkennbar, in welcher Richtung dieser scheinbare Angriff stattgefunden hat. Detaillierte Informationen sind mit einem Maus-Klick auf den „Threat/Content Namen“ verfügbar.

Der Bereich „Data Filtering“ klassifiziert die Top 5 Dateitypen, die als Nutzdateninhalte übertragen wurden.

Das ACC stellt damit einen guten Überblick über die aktuelle Situation im Netzwerk zur Verfügung, von dem aus man mit weiteren Klicks in die detaillierte Analyse einsteigen kann.

Alle dargestellten Bereiche können als Entscheidungsgrundlage für eine Sicherheits-Policy genutzt werden. Das bedeutet, dass Regelwerke der folgenden Art erstellt werden können:

Aus den Institutsnetzen des JuNet in das weltweite Internet ist Web-browsing erlaubt, falls keine Adobe Portable Document Format (PDF) Dateien übertragen werden; Netzwerkverkehr dieser Art wird durch das IPS-System und den Viren-Scanner analysiert.
Aus Institutsnetz A ist die Übertragung von MS Office in das Netz der Partnerinstitution P gestattet; Netzwerkverkehr dieser Art wird vom Viren-Scanner analysiert
Verbiete die Übertragung von Microsoft Office Dateien.

Sicherheits-Policies werden auf dem Gerät also nicht nur auf Basis von IP-Adressen und Ports konfiguriert. Vielmehr sind die Regelwerke aus einzelnen Bausteinen zusammengesetzt, welche die Funktionalität als UTM-System widerspiegeln.

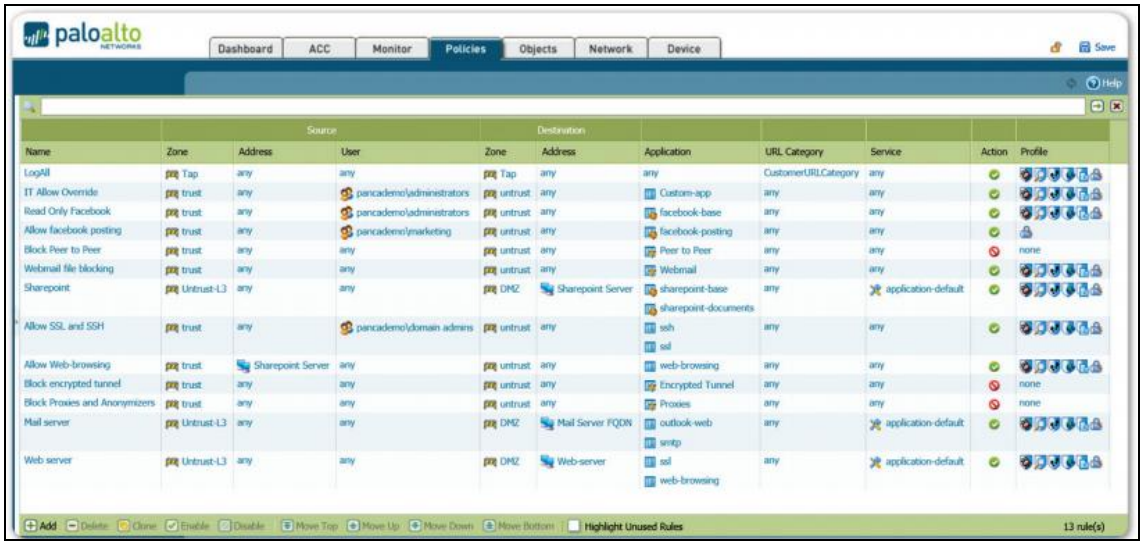

Abbildung 11: Policies der Palo Alto

Abbildung 11 zeigt eine Beispiel-Policy. Alle Spalten, außer „Action“ und „Profile“, stellen Entscheidungsfindungskriterien dar, auf deren Basis dann die „Action“ ausgeführt wird. In der Spalte „Profile“ werden zusätzliche Sicherheits-Features zur Policy hinzugefügt. Dazu zählen z.B. Threat-Detection (IDS/IPS) und Antivirus.

In Abbildung 11 sind die Zonen „trust“ und „untrust“ als Quelle oder Ziel markiert. Diese beiden Zonen sind standardmäßig definiert und stellen die am meisten schützenswerte interne Zone und am wenigsten schützenswerte externe Zone dar. Weitere Zonen zur Segmentierung des Netzwerks können definiert werden. So kann z.B. auch Verkehr zwischen Organisationseinheiten auf dem Campus analysiert werden, wenn das Gerät an der richtigen Stelle im Netzwerk platziert wird.

Während der Tests zeigte die Palo Alto PA-5020 eine gute Erkennungsrate von möglichen Angriffen und Malware-Infektionen auf Basis der Threat-Signaturen, da keine Fehlalarme generiert wurden. Das System verfügte zum Testzeitpunkt nicht über eine Anomalieerkennug. Das bedeutet, dass zur Erkennung evtl. Threats in kryptographisch gesicherten Verbindungen der Klartext vorliegen muss. In anderen Worten: Die Verschlüsselung muss auf dem Gerät aufgebrochen werden. Laut den Anforderungen aus Kapitel 2 ist das zurzeit im JuNet nicht gewünscht. Im Allgemeinen sind die Alarme in der Detailanalyse gut erklärt und für den Analysten nachvollziehbar. Über fest definierte Signaturen des Herstellers hinaus können benutzerdefinierte Regeln erstellt werden. Signaturen zur Applikationserkennung können nur in Absprache und Zusammenarbeit mit dem Hersteller erstellt werden.

Die topologischen Anforderungen an das System können erfüllt werden. Würde das Campusnetzwerk so segmentiert, dass Netzbereiche der Organisationseinheiten einzelne Zonen der Policy bildeten, könnte der Netzwerkverkehr in jede und aus jeder beliebigen Kommunikationsrichtung analysiert werden. Die verwendete Protokollfamilie auf Layer 3 (IPv4 oder IPv6) spielt dabei keine Rolle, da das Testgerät sowohl Angriffe über beide erkennt als auch über beide administriert werden kann. Eine Korrelation der Angriffe über IPv4 und IPv6 ist dann theoretisch möglich, da das System als lokales Gateway in jedem Netz über entsprechende Zusatzinformationen (Hardware-Adresse, etc.) verfügt. In jedem anderen Fall kann die Korrelation nur durch zusätzliche Werkzeuge und

Hilfsmittel erfolgen. Weil Syslog gesendet werden kann, könnte diese Korrelation auf dem Splunk>-Cluster des JSC erfolgen.

Das System verfügt seit der Version 5.0 über eine XML-API[9]. Sie erlaubt lesenden und schreibenden Zugriff auf die Konfiguration des Systems, so dass unterschiedliche Prozesse im Rahmen der Administration und Konfiguration automatisiert werden können.

Das System unterstützt agentless Monitoring über SNMP und kann somit in die bestehende Monitoring-Infrastruktur eingebunden werden. Allerdings ist die Integration in ein zentrales Management nur mit notwendigen Anpassungen möglich.

Die Anforderungen sind damit im Wesentlichen gut abgedeckt. Abstriche gibt es bei der Palo Alto aus zwei Gesichtspunkten: Das Testsystem PAN-5020 verfügte, wie oben erwähnt, nicht über den für das JuNet notwendigen Durchsatz von 10 Gb/s, war aber zur Verifikation der Testanforderungen vollkommen ausreichend. Das passende Palo Alto System mit einem Mindestdurchsatz von 10 Gb/s (PA-5060) überschritt aber deutlich das verfügbare Budget. Aufgrund der Gerätekonzeption als UTM-System und dem Einsatz an einem zentralen Punkt des Netzwerkes, müsste das System als High-Availability-Lösung in das JuNet integriert werden.

Der zweite Abstrich muss aufgrund der Hardware-Architektur des Gerätes gemacht werden. Palo Alto Geräte basieren sehr stark auf anwendungsspezifischen integrierten Schaltungen (Application Specific Integrated Circuit, ASIC[10]), so dass Schwachstellen im Vergleich zu software-basierten Systemen schwieriger zu beheben sind, da im schlimmsten Fall komplette ASICs getauscht werden müssten.

4.2 Fortinet

Fortinet Inc. wurde im Jahr 2000 von den Brüdern Ken und Michael Xie gegründet. Ken Xie war 1997 einer der Gründer von NetScreen, deren Schwerpunkt ASIC-basierte Firewall und Intrusion Detection Systeme waren. Der Börsengang des Unternehmens erfolgte im Jahr 2009.

Als Testgerät wurde eine FortiGate-800c bereitgestellt. Sie bietet 20 Gb/s Firewall-Durchsatz, 6 Gb/s Intrusion-Prevention-Durchsatz und ansonsten alle Funktionalitäten größerer Modelle, die von den Performance-Daten her eher für einen Einsatz im JuNet geeignet wären.

Das System wird über eine Web-Schnittstelle administriert und konfiguriert. Nach dem erfolgreichen Login wird eine Übersichtsseite angezeigt, vgl. Abbildung 12. Im linken Randbereich der Seite befinden sich alle Funktionen zur Administration sortiert. Im Hauptteil der Web-Seite wird eine Übersicht über den Systemstatus gegeben. Die beiden Zeiger rechts oben zeigen die CPU-Nutzung und die Speicherauslastung des

[9] https://live.paloaltonetworks.com/servlet/JiveServlet/downloadBody/4126-102-7-23074/XML-API-5.0.pdf

[10] http://de.wikipedia.org/wiki/Anwendungsspezifische_integrierte_Schaltung

Systems an. Unten links ist ein Widget eingeblendet, dass den direkten Konsolenzugang zum System ermöglicht.

Abbildung 12: Fortigate Webschnittstelle

Ein Fortigate-System kann je nach Modell in bis zu 500 virtuelle Firewalls aufgeteilt werden. Jede virtuelle Firewall verfügt über ein Set von Interfaces, über welche Netzwerkverkehr weitergeleitet wird. Jede virtuelle Firewall verfügt über eine eigene Policy. Kommunikationsbeziehungen werden dabei immer zwischen Zonen angegeben.

Die eigentliche Konfiguration der Policy und die gesamte Architektur ähnelt stark dem Palo Alto Ansatz. Auch bei der Fortigate UTM-Lösung basieren die Entscheidungskriterien des Regelwerkes im Wesentlichen auf der Applikationserkennung, Benutzernamen und Kommunikationsrichtung. Jede Regel kann durch Profile wie IDS/IPS, Antivirus und URL-Filter ergänzt werden.

Aufgrund der großen Ähnlichkeit zur Palo Alto Konfigurationsoberfläche wird an dieser Stelle auf eine weitere Beschreibung der Konfiguration verzichtet.

Das System fiel im Test durch seine äußerst benutzerfreundliche Konfigurationsoberfläche auf. Sie ist klar strukturiert und einfach zu bedienen.

Die Angriffserkennung der Fortigate 800C produzierte während der Tests eine Vielzahl von Alarmen, deren Nachvollziehbarkeit schwerer war als bei der Palo Alto Lösung. Die vorgegebenen Signaturen des Systems sind in verschiedene Klassen eingeteilt, diese Klassen können entweder aktiviert oder deaktiviert werden. Das bedeutet, dass eine Signaturklasse, die Angriffe auf Microsoft Excel signalisiert, das gesamte Versionsspektrum der Software abdeckt und Alarme für Angriffe auf Excel 95 gemeldet werden. Da einzelne Signaturen nicht deaktiviert werden können, sind Fehlalarme vorprogrammiert. Darüber hinaus sind angezeigte Alarme nicht immer ausreichend nachvollziehbar erklärt. Die Beschreibung des Alarms liefert keine hinreichenden Details zur Erklärung, warum der jeweilige Alarm angezeigt wird.

Da das System ebenso wie die Palo Alto Lösung nicht über eine Anomalieerkennung verfügt, muss zur Erkennung von Threats in kryptographisch gesicherten Verbindungen der Klartext vorliegen. Wie bereits bei der Beschreibung des Palo Alto Systems erwähnt, ist diese Lösung zurzeit im JuNet nicht angedacht. Über fest definierte Signaturen des Herstellers hinaus können benutzerdefinierte Regeln erstellt werden. Signaturen zur Applikationserkennung können nur in Absprache und Zusammenarbeit mit dem Hersteller erstellt werden.

Alle Testanforderungen werden vom System in gleichem Maße erfüllt wie von der Palo Alto Lösung. Das System analysiert IPv4 und IPv6 Verkehr auf mögliche Angriffe, es kann über beide Protokollfamilien administriert werden. SNMP-Monitoring und Syslog werden unterstützt, so dass die Integration in das bestehende Monitoring und Splunk>-Cluster ohne weiteres möglich ist. Allerdings muss das zentrale Management wie auch beim Palo Alto System entsprechend angepasst werden.

Das Fortinet-System überzeugte im Test nicht nur mit einer klar strukturierten Benutzeroberfläche, sondern auch als Next-Generation-Firewall. Im Bereich der Intrusion-Prevention und –Detection müssen aber Abstriche gemacht werden. Aufgrund der nicht immer vollständig gegebenen Nachvollziehbarkeit der Alarme und der wenig granularen Konfigurationsmöglichkeiten bei der Aktivierung der Signaturen konnte das System nicht überzeugen.

Auch die Fortinet Geräte basieren sehr stark auf ASICs, so dass Schwachstellen im Vergleich zu software-basierten Systemen schwieriger zu beheben sind, da im schlimmsten Fall komplette ASICs getauscht werden müssten. Auch hier besteht eine große Ähnlichkeit zu Palo Alto. Allerdings sind die Fortinet-Systeme in der Anschaffung wesentlich günstiger. Daher sollte bei einer Erneuerung des zentralen Firewall-Clusters sicherlich eine erneute Untersuchung mit Fortinet stattfinden.

4.3 Sourcefire

Sourcefire Inc. wurde im Jahr 2001 von Martin Roesch gegründet. Roesch war Entwickler des Open-Source-IDS Snort. Sourcefire bemüht sich daher stark um die Weiterentwicklung Snorts und pflegt eine enge Beziehung zur Snort-Benutzergemeinschaft. Neben Snort wird auch ClamAV als unixoide Antivirenlösung von Sourcefire unterstützt. Im März 2007 erfolgte der Börsengang und Ende 2014 erfolgte die Übernahme durch Cisco.

Das Sourcefire System besteht aus zwei Komponenten. Getestet wurde eine firePOWER 3D8350 mit 15 Gb/s Intrusion-Prevention-Durchsatz und 30 Gb/s Firewall-Durchsatz. Die firePOWER Serie kann als IDS, IPS, Next Generation Firewall, URL-Filter und UTM-System eingesetzt werden.

Administriert und konfiguriert werden firePOWER–Geräte, die im klassischen IDS/IPS-Sprachgebrauch als Sensoren bezeichnet werden, über das fireSIGHT Defense Center. Das Defense Center, kurz DC, ist eine eigene Appliance, die bis zu 150 Sensoren verwalten kann. Das DC des Testsystems war eine DC3500 mit 12 GB RAM und 400

GB Event Storage. Das bedeutet, die Alarmdatenbank des Systems kann maximal 400 GB fassen.

Die Administration erfolgt über die Web-Schnittstelle des Defense Centers (Abbildung 13). Wie bei allen Testsystemen wird auch hier eine Übersicht über den aktuellen Zustands des Netzwerks angezeigt. Die angezeigten Widgets sind frei definierbar und können individuell angepasst werden. Das zweite Widget von oben in der linken Spalte zeigt die Anzahl erkannter unterschiedlicher Applikationen. Das in der rechten Spalte zweite Widget von oben listet die TOP 10 der erkannten Betriebssysteme auf. Vorteilhaft ist, dass alle diese aus dem analysierten Netzwerkverkehr gewonnenen Informationen in die Firesight Datenbank einfließen und bei zukünftigen Entscheidungen über vermeintliche Angriffe auf ein System als Entscheidungsgrundlage genutzt werden.

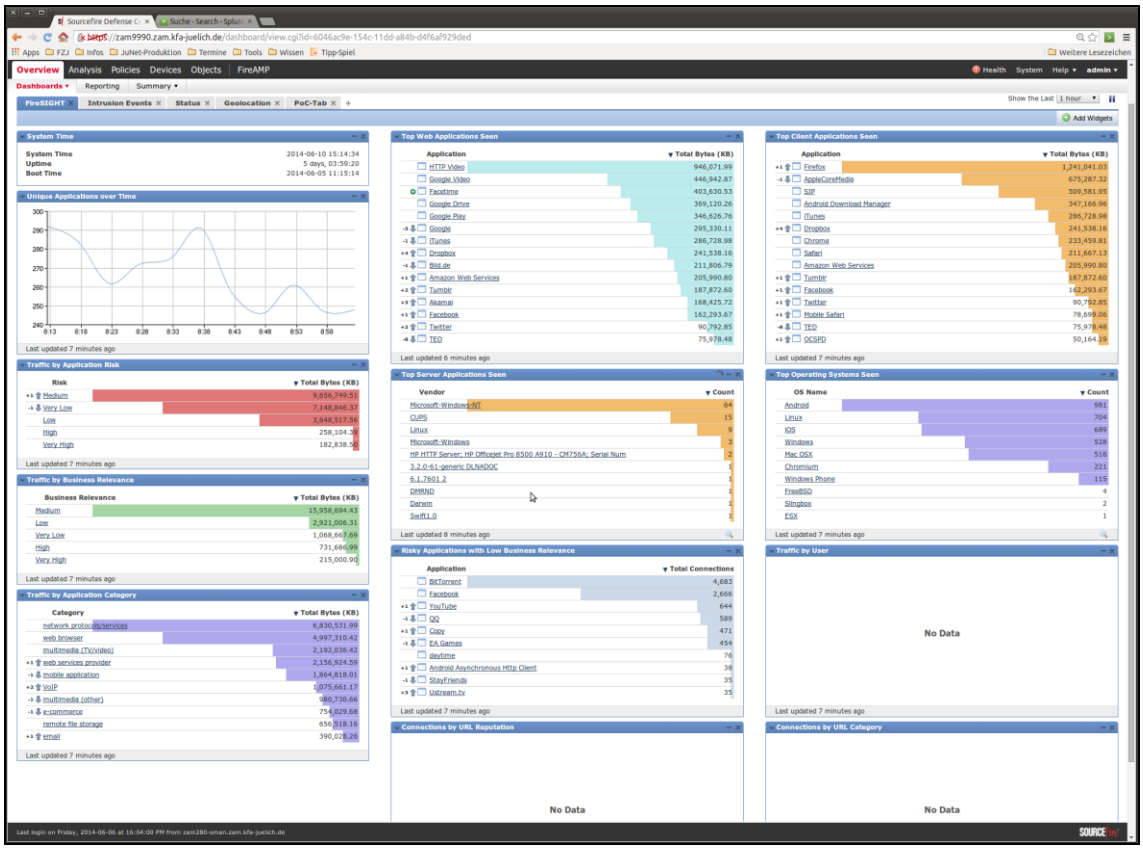

Abbildung 13: Sourcefire Defense Center

Insbesondere erstellt das Sourcefire Gerät Hostprofiles, vgl. Abbildung 14. Der primäre Schlüssel dieser Information ist die IP-Adresse des Hosts, so dass in einem dynamischen Umfeld wie dem Wireless LAN des Junet die Informationen weniger hilfreich sind als im kabelgebundenen Campusnetzwerk, wo Rechner eine feste IP-Adresse erhalten. Im kabelgebundenen Netz wird sich mit längerer Betriebsdauer ein sehr genaues Profil des jeweiligen Rechners ergeben.

Das Hostprofile besteht im oberen Bereich aus allgemeinen Informationen. Im Bereich View werden verschiedene Links angezeigt, die dem Administrator des Intrusion Prevention Systems die Möglichkeit bieten, eine detaillierte Analyse von Events und Alarmen, die in Verbindung mit diesem Host stehen, durchzuführen.

Darunter werden das Betriebssystem, seine Version und die Quelle der Information angezeigt. FireSIGHT bedeutet in diesem Kontext, dass alle Informationen aus dem analysierten Netzwerkverkehr gewonnen wurden. Hier bietet das System eine API an, so dass Informationen aus Schwachstellen-Scans und Patch-Management-Systemen mit eingebunden werden können.

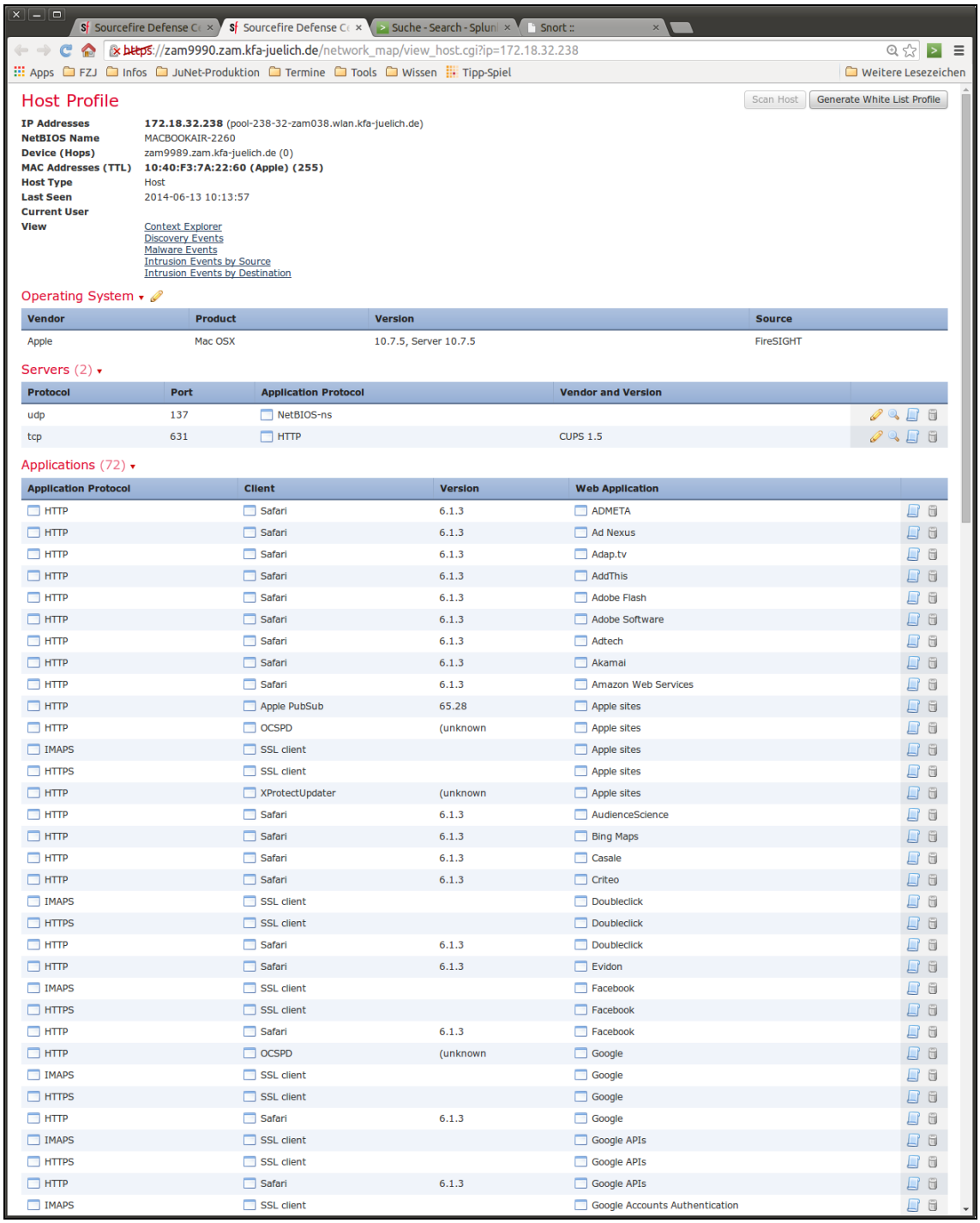

Abbildung 14: Firesight Hostprofile

Nach dem Betriebssystem werden alle Applikationen aufgelistet, für die der Rechner als Server angesprochen wurde und alle Applikationen, die als Client genutzt wurden.

Aufgrund der Versionsnummern der genutzten Applikationen ergibt sich so die Möglichkeit etwaige Angriffe besser zu bewerten. Das bedeutet im angezeigten Beispiel, dass ein Angriff auf Version 5 des Safari-Webbrowsers hier nicht relevant ist und daher nicht angezeigt bzw. nicht gemeldet wird.

Oberhalb der Widgets in Abbildung 13 werden fünf Tabellenreiter angezeigt, die weitere Übersichten liefern. Der zweite Reiter liefert eine Übersicht über Alarme im Bereich Intrusion Detection und Prevention. Hier überzeugte das Sourcefire System deutlich im Vergleich zu anderen Testsystemen. In der Detailanalyse konnte bei jedem Alarm nachvollzogen werden, warum der Alarm angezeigt wurde. Die Benutzeroberfläche ist klar und deutlich strukturiert und führt direkt ohne große Eingewöhnungszeit zu den gewünschten Ergebnissen.

Ein wesentlicher Vorteil dieses Gerätes sind vordefinierte Regelwerke für Intrusion Detection bzw. Intrusion Prevention. In der Einstellung „Security over Connectivity“ ist die größte Anzahl an Signaturen aktiviert. Die Anforderungen bzgl. der Integrität des zu schützenden Netzwerks stehen darin über den Anforderungen der Benutzer nach möglichst reibungsloser, freier Netzwerkkommunikation. Im Gegensatz dazu steht die Policy „Connectivity over Security“. Hier wird der Zugriff auf Ressourcen möglichst weit eingeräumt und nur wenige Signaturen sind eingeschaltet. Der Mittelweg zwischen beiden ist die Policy „Balanced Security and Connectivity“.

Diese Standardregelwerke bieten eine exzellente Ausgangsbasis bei der Inbetriebnahme eines IPS. Ausgehend von einem der Regelwerke kann die Anpassung an die jeweilige Netzwerkumgebung erfolgen. Zusätzlich unterstützen die Informationen aus der FireSIGHT-Datenbank die Analyse und die Alarmierung. Zusätzlich zu den definierten Signaturen können benutzerdefinierte Signaturen erstellt werden, vgl.Abbildung 15.

Zusätzlich zur signaturbasierten Erkennung verfügt die firePOWER-Serie auch über eine Anomalieerkennung, die aber in den vorliegenden Tests aufgrund des dynamischen Charakters des Wireless LANs nicht näher betrachtet wurde.

Damit erfüllt die Sourefire alle Anforderungen zur Angriffserkennung bestens. IPv4 und IPv6 werden sowohl im Bereich Management als auch im Bereich der Angriffserkennung unterstützt.

Die Anforderungen an die Topologie erfüllt die firePOWER ebenfalls bestens. Das System verfügt als einziges der Testsysteme über einen sog. Fail-Open-Modus. Das bedeutet, dass obschon das Gerät im Netzwerkverkehr aktiv eingebunden ist, bei einer möglichen Störung eine direkte Überbrückung möglich ist und der Netzwerkverkehr nicht betroffen ist. Ferner kann das System auch als IDS-System eingesetzt werden und passiv den Verkehr analysieren.

Das System kann Alarme und andere Systemzustände per Syslog an einen Server schicken. Die Integration in das bestehende Splunk>-Cluster des JSC funktioniert problemlos. Wie bereits weiter oben erwähnt, existiert eine API, über die sowohl Informationen ausgelesen als auch zusätzlich eingepflegt werden können.

Eine Einbindung in das bestehende Monitoring ist problemlos möglich. Aufgrund der Tatsache, dass Sourcefire eine Tochterfirma der Cisco Systems Inc. ist, ist zu erwarten, dass das IPS-System zukünftig nahtlos in ein zentrales Cisco Management Systems eingebunden werden kann.

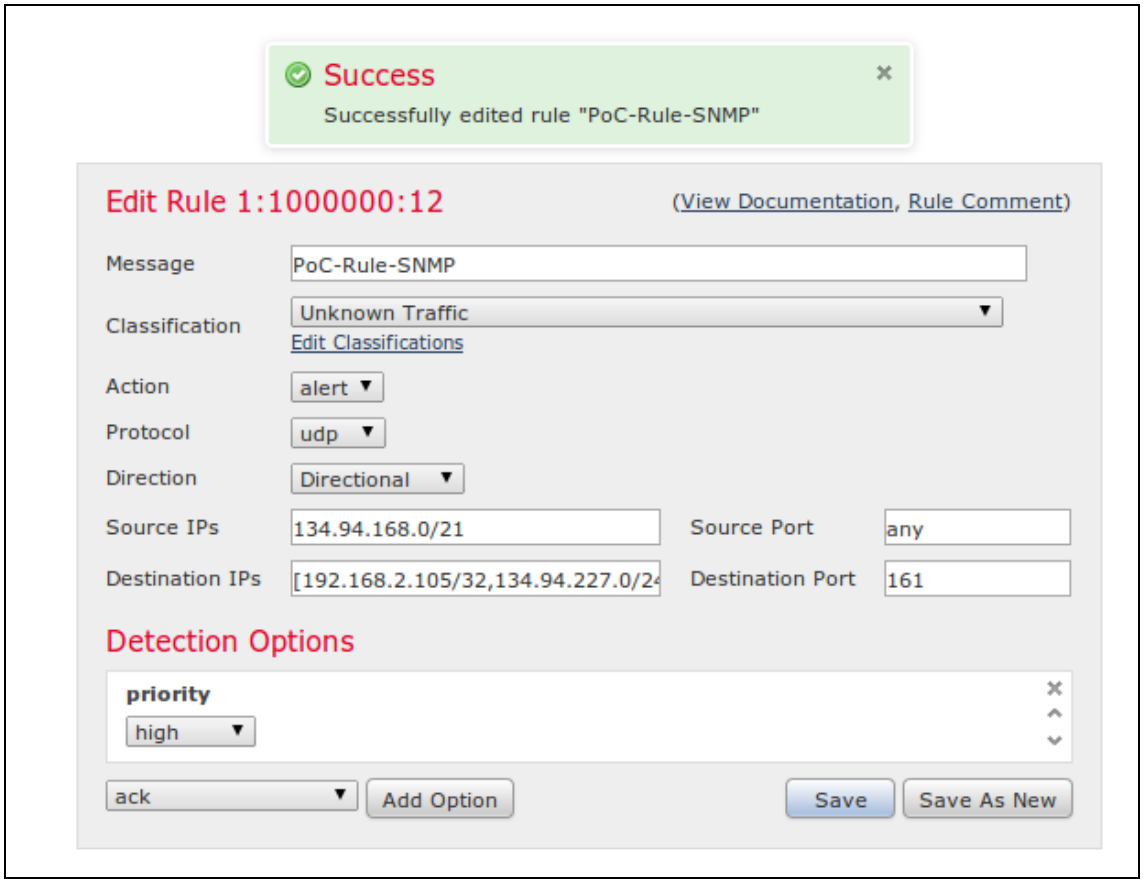

Abbildung 15: Benutzerdefinierte Signatur erstellen

4.4 Lancope

Lancope wurde im Jahr 2000 als Spin-Off des Georgia Institute of Technology gegründet. Das Produkt Stealthwatch analysiert Netflow-Informationen mit dem Schwerpunkt auf Anomalieerkennung, um so eventuelle Angriffe zu erkennen. Die Lancope Lösung ist ein wesentlicher Bestandteil der Cisco System Cyber Threat Defense Solution[11].

Bevor die Lancope-Lösung beschrieben wird, muss zuerst Netflow erklärt werden. Netflow ist eine Technologie von Cisco Systems Inc., die auf Layer 3 und Layer 2 Geräten (Router, Switches) eingeführt wurde. Netflow generiert Informationen über einen IP-Datenstrom, der über ein IP-Interface empfangen oder gesendet wurde. Mittlerweile wird die Technik von vielen Herstellern unterstützt. Neben Cisco‘s Netflow existieren noch andere Standards, unter anderem der herstellerunabhängige

[11] http://www.cisco.com/web/strategy/docs/gov/cyber_threat_defense_so.pdf

Standard IPFIX, der in RFC 3917[12] beschrieben ist. Mindestens enthält eine Netflow-Information einen Zeitstempel, die IP-Adressen, TCP bzw. UDP Ports, sowie Byte- und Paketzähler. Diese Informationen werden passiv erhoben – ohne den eigentlichen Netzwerkverkehr zu beeinflussen - und periodisch an einen NetFlow-Collector gesendet.

Der NetFlow-Collector aggregiert die empfangenen Flow-Informationen. Die zusammengefassten Flows entsprechen damit einem Einzelverbindungsnachweis auf der Telefonrechnung. Man erkennt schnell und einfach wer mit wem, wann, wie lange und wie viel kommuniziert hat. Der ursprüngliche Schwerpunkt der NetFlow-Technik lag in der Verkehrsanalyse und der Kapazitätsplanung. Die notwendige Analyse kann durch den Flow Collector oder eine weitere Analysekomponente erfolgen.

Das Lancope Produkt StealthWatch besteht aus drei verschiedenen Komponenten. Die zentrale Komponente bildet der StealthWatch Flow Collector. Er empfängt die Netflow Informationen verschiedener Quellen und aggregiert diese. Die StealthWatch Management Console (SMC) stellt die Analysekomponenten und Benutzerschnittstelle dar. Die dritte Komponente ist der StealthWatch Flow Sensor, der NetFlow auf Basis des IPFIX-Standards generiert und Nutzdaten des IP-Datenstroms analysiert.

Neben Verkehrsanalyse und Kapazitätsplanung analysiert das Lancope Produkt die NetFlow-Informationen unter Gesichtspunkten der Intrusion Detection. Das Produkt ist generell anomaliebasiert.

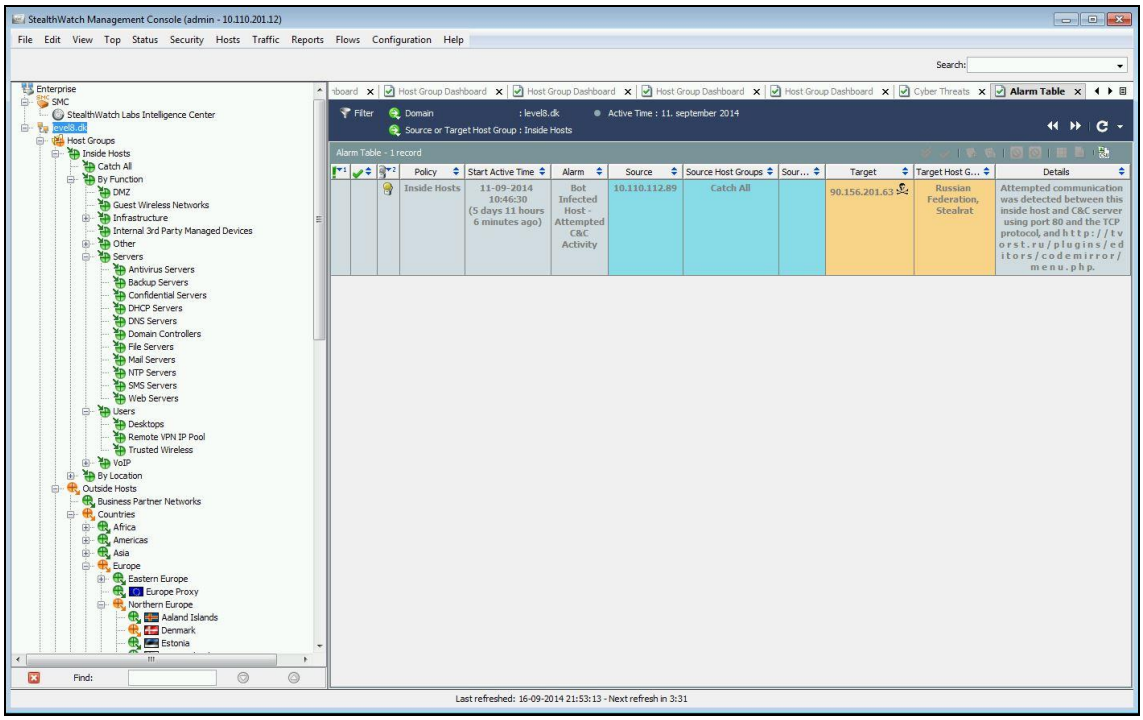

Abbildung 16: StealthWatch Management Console[13]

[12] http://tools.ietf.org/html/rfc3917

[13] https://www.level8.dk/wp-content/uploads/2014/09/SMC-2.jpg

Nach der Inbetriebnahme werden sog. Host-Groups angelegt, die im linken Teil der Abbildung 16 dargestellt sind. Hier spiegelt sich im Wesentlichen die Netzstruktur wieder. Generell existieren drei vordefinierte Gruppen: inside, outside und catch all. Alle IP-Adressen, die am Netz gesehen worden sind und einer Gruppe zugeordnet werden können, fallen in die Gruppe „catch all“. Die „inside“ und „outside“ Gruppen entsprechen ihrer Namensgebung.

Diese beiden Gruppen spannen je einen Baum für Host-Gruppen auf. Innerhalb eines Baumes wird die Policy von Vaterknoten auf die Kinder vererbt. Hat ein Knoten eine vom Vater abweichende Policy, so wird die Policy des Vaterknotens nicht beachtet. In der umgekehrten Richtung werden die Inhalte und Alarme der Host-Gruppen von den Kindknoten auf die Elternknoten übertragen, so dass nur die Blätter eines Host-Gruppen-Baumes mit den entsprechenden Adressen gefüllt werden.

Direkt ab der Inbetriebnahme beginnt die StealthWatch Lösung mit dem sog. Profiling. Das bedeutet, dass zunächst ein Basisprofil für das Verhalten einzelner Rechner erstellt werden muss. Diese Basis wird fortlaufend im Betrieb angepasst und erneuert. Bei Abweichungen von dieser Basis werden dann Alarme des Systems generiert.

Diese Funktionalitäten gewährleistet das Produkt auf Basis der NetFlow-Daten der bestehenden Netzwerkinfrastruktur. Alle im JuNet eingesetzten Komponenten bieten die technischen Voraussetzungen, NetFlow an einen FlowCollector senden zu können.

Verbessert wird die Analyse durch den StealthWatch Flow-Sensor. Wie bereits oben erwähnt, sendet der StealthWatch Flow-Sensor Informationen auf Basis des IPFIX-Standards. Der Flow-Sensor arbeitet als Deep-Packet-Inspection Instanz, die Nutzdaten analysiert und daraus Informationen generiert, z.B. welche Applikation genutzt wird. Ein weiteres Feature ist die Erkennung von sog. Botnet-Traffic. Dazu werden Muster bekannter Bots gegen den Nutzdatenteil abgeglichen.

Das Testsystem wurde nicht nur im W-LAN getestet. Der Flow-Collector sammelte Informationen verschiedener Systeme. So wurden einzelne Ethernet-Broadcast-Domänen betrachtet, die NetFlows des zentralen Firewall-Clusters und die NetFlows des internen IPv6-Routers.

Während der Testphase wurde deutlich, dass die anomaliebasierte Angriffserkennung zur Erkennung von Innentätern wenig praktikabel ist. Das Verhalten der JuNet-Clients ist extrem dynamisch und verändert sich täglich, so dass permanente Anpassungen notwendig wären. Außerdem ist die Struktur in den Netzwerken der Organisationseinheiten nicht an zentraler Stelle bekannt, z.B. kann ein System heute als Client in der JuNet-Datenbank angemeldet werden und morgen ein Server mit einer Firewall sein, so dass das Host-Gruppen-Profile angepasst werden müsste. Diese Änderungen sind aber schwer nachzuvollziehen und automatisiert noch nicht zu leisten.

In der Erkennung externer Angreifer und möglicher Angriffe auf externe Hosts liefert das System aber einen großen Beitrag. Port- und Hostscanner werden zuverlässig erkannt und können automatisiert an zentraler Stelle gesperrt werden. Damit könnte StealthWatch die bisher eingesetzte Eigenentwicklung ablösen und verbessern, da für die Eigenentwicklung eine Anpassung an neue Verkehrsmuster erfolgen muss.

Weitere Vorteile bietet das System in der Analyse von Sicherheitsvorfällen. Beispielsweise können Alarme eines anderen IPS-Systems mit den NetFlow-Daten detailliert abgeglichen werden.

Außerdem bietet Lancope eine API an, die das Auslesen und Setzen von Einstellungen und Aktionen erlaubt.

Betrachtet man die Anforderungen aus Kapitel 2, so kann StealthWatch keine bekannten Angriffe erkennen, da es ein rein anomaliebasiertes System ist. Die topologischen Anforderungen sind voll erfüllt, da die Informationen aus der Netzwerkinfrastruktur gewonnen werden, die die Topologie des JuNets aufspannt. So sind auch die Protkolle IPv4 und IPv6 für das System vollkommen invariant in der Anwendung der Analysealgorithmen. Lediglich die Integration in ein zentrales Management ist nicht möglich.

4.5 Auswahl des zu beschaffenden Systems

Aufgrund der durchgeführten Tests und der gewonnenen Erfahrungen ist das Sourcefire firePOWER-System als IDS/IPS für JuNet am besten geeignet. Ausschlag gebend für diese Empfehlung sind neben der sehr guten Bedienbarkeit auch die vielfältigen Möglichkeiten der Integration in das JuNet und die Erweiterbarkeit an zukünftige Anforderungen. Des Weiteren ist es möglich, die Alarmierung über erkannte Angriffe per Syslog an das Splunk>-Cluster des JSC zu senden und von dort aus automatisierte Aktionen durchzuführen.

Gleichzeitig wird aber auch die zusätzliche Anschaffung eines Lancope StealthWatch-Systems favorisiert, da es die bestehende Eigenentwicklung direkt ersetzen und verbessern kann. Alarme des Systems können ebenfalls per Syslog in das Splunk>-Cluster exportiert werden. Darüber hinaus können die Vorteile bei der Analyse eines Alarms oder Vorfalls zusätzlich in das Splunk>-Cluster integriert werden, so dass weitere Arbeitsschritte automatisiert ablaufen können, die dann wiederum Aktionen und Konfigurationen über die API an das Lancope-System schicken können.

Abbildung 17 zeigt ein Beispiel, wie die Integration aussehen kann. Im aufgeklappten Kontextmenü sind „GetFlow“-Aktionen ausführbar, die Informationen aus dem Flow-Collector auslesen und bereitstellen.

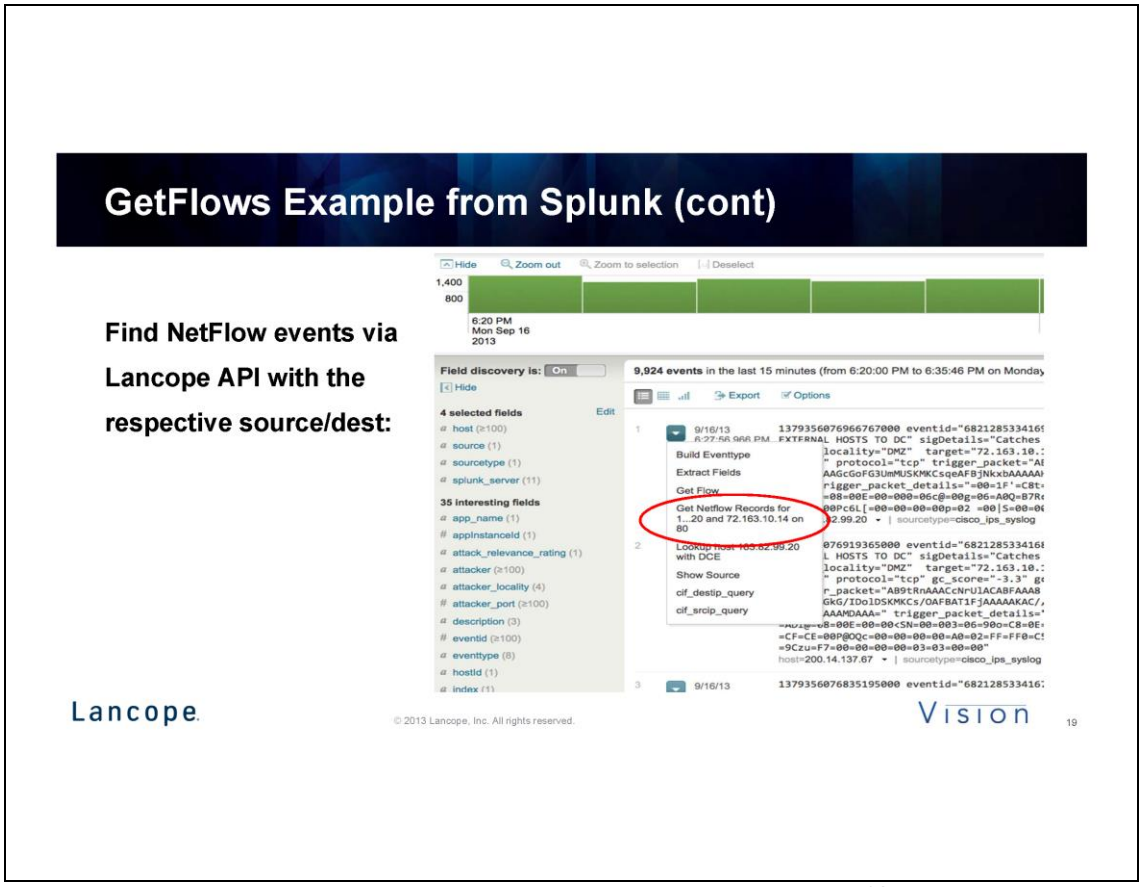

Abbildung 17: Integration Lancope Splunk>[14]

In der folgenden tabellarischen Zusammenfassung sind die Testergebnisse zu den gestellten zusammengefasst. Die letzte Zeile „Anschaffungspreis“ bezieht dabei nicht auf die getesteten Systeme, sondern auf diejenigen, die für den Einsatz im JuNet ausgewählt worden wären, und ist ein ungefähre Angabe der Preislisteninformation.

[14] Quelle: Paul Eckstein, Heather Pegram (Cisco CSIRT Engineers) „Incident Response with StealthWatch and 13B Flows per Day“, Lancope User COnferent Atalanta, 15.-17.10.2013

Testgerät \ Anforderung	Palo Alto PA-5020	Fortinet FortiGate-800c	Sourcefire firePOWER 3D8350	Lancope Stealthwatch
Bekannte Angriffe erkennen	++	+	++	0
Unbekannte Angriffe erkennen	0	0	+	+
Kann als Man in the middle eingesetzt werden	++	++	0	0
Topologische Anforderung: Möglichst verteilter Einsatz	+	+	++	++
IPv4 wird analysiert	++	++	++	++
IPv6 wird analysiert	++	++	++	++
Korrelation IPv4 u IPv6 möglich	0	0	0	+
System sendet Alarm per Syslog	+	+	++	+
System besitzt eine API	+	+	++	++
Management über IPv6	++	++	++	++
Integration in zentrales Monitoring	++	++	++	++
Integration in zentrales Management	--	--	+	0
Anschaffungspreis	ca. 550.000 €	ca. 450.000 €	ca. 330000 €	ca. 100.000 €

5. Einsatzszenario

In diesem Kapitel soll beschrieben werden, wie die ausgewählte Lösung in das JuNet integriert werden kann. Abbildung 18 zeigt eine schematische Darstellung.

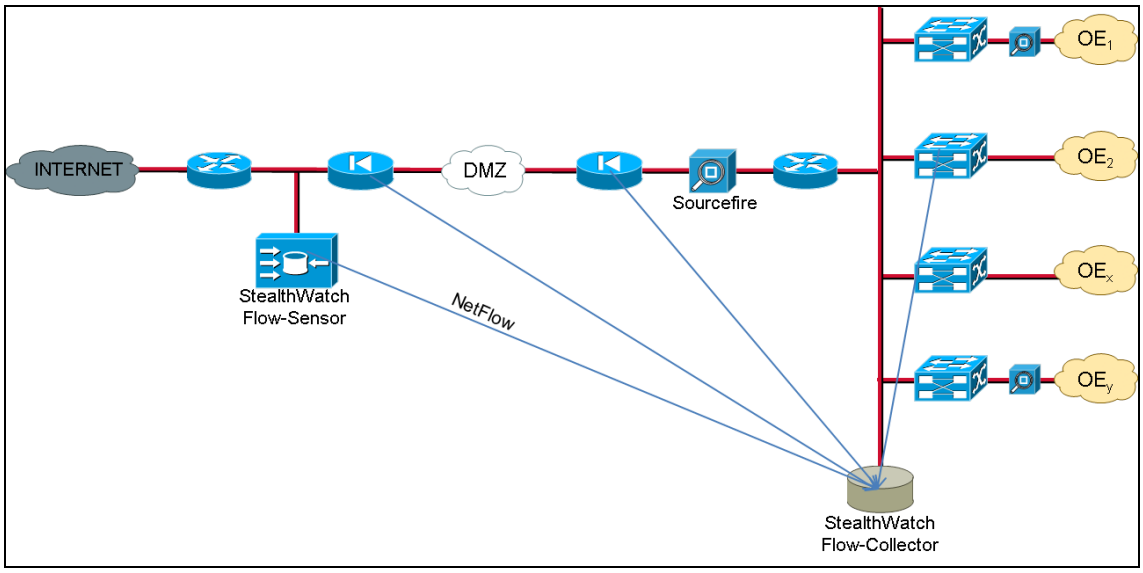

Abbildung 18: Einsatzszenario

Zunächst soll der Einsatz der Sourcefire Komponente erläutert werden. In der schematischen Darstellung sind Clients mit hohem Schutzbedarf im internen Netz hinter den Firewalls eingesetzt, so dass genau dort ein performanter Sensor als IPS-System plaziert wird. Hier können Angriffe von und nach extern verhindert werden. Abgesetzte Sensoren können je nach Bedarf und Anforderung in kleineren Segmenten als passiver Sensor (Intrusion Detection) oder auch als aktiver Sensor (Intrusion Prevention) eingesetzt werden. Generell ist zu beachten, dass die Sourcefire-Komponenten als aktive Sensoren immer im Modus Fail-Open betrieben werden, so dass bei einem Ausfall des Systems der Netzwerkverkehr nicht beeinträchtigt wird. Generell soll die Sourcefire-Lösung nur diejenigen Angriffe unterbinden, die nicht von der zentralen Firewall verhindert werden.

Die Lancope-Komponenten werden so eingesetzt, dass der Flow-Collector im internen Netz NetFlows von ausgewählten Komponenten der Netzwerkinfrastruktur empfängt. Hier sollen nach Möglichkeit Host- und Portscanner erkannt werden und Informationen für nachträgliche Analysen gewonnen werden.

Der Flow-Sensor soll vor der externen Firewall eingesetzt werden. Dadurch werden z.B. Host- und Port-Scanner frühzeitig erkannt, da alle Flow-Informationen – auch die von der Firewall geblockten – zur Verfügung stehen. Zusätzlich kann der Sensor Bot-Traffic erkennen, der nicht von anderen zentralen Geräten unterbunden würde. Gleichzeitig stehen durch die Vielzahl der Flows weitere Analysemöglichkeiten bei der Untersuchung eines Vorfalls zur Verfügung, so dass im Rahmen forensischer Arbeiten ein genaueres Bild eines Angriffs gezeichnet werden kann.

6. Ausblick

Die Auswahl der Sourcefire- und Lancope-Lösungen im Rahmen der Anschaffung eines IDS/IPS für JuNet stellt eine zukunftssichere Lösung dar. Bekannte und unbekannte Angriffe können auf Basis der unterschiedlichen Erkennungsalgorithmen erfasst und bearbeitet werden. Dabei spielt die Version des Internet Protokolls (IPv4 oder IPv6) keine Rolle, da beide Systeme beide Protokollfamilien analysieren können.

Sourcefire liefert mit der firePower und fireSIGHT eine Lösung, die nicht nur die notwendige Performance-Anforderung erfüllt, sondern auch auf die Umgebung im JuNet angepasst werden kann. Außerdem kann das System auf maximal 45 Gb/s IPS-Durchsatz ausgebaut werden. Da Sourcefire ein Tochterunternehmen von Cisco Systems ist, kann die Verfügbarkeit am Markt und der weitere Ausbau mit hoher Wahrscheinlichkeit angenommen werden.

In einer der ersten Ausbaustufen gilt es außerdem, Informationen von Schwachstellen-Scannern und Patch-Management-Systemen in das IPS zu integrieren, damit eine eventuelle Alarmierung bezüglich eines JuNet-Systems genauestens abgestimmt ist. Die Integration dieser Informationen kann über kommerzielle Systeme oder durch Eigenentwicklungen erfolgen.

Die Lancope-Komponenten integrieren Informationen der bestehenden Netzwerkinfrastruktur in den Sicherheits-Prozess des Forschungszentrums. Sie bieten die Möglichkeit direkt mit der Infrastruktur im JSC (Splunk>-Cluster) zu interagieren. Alarme können an Splunk> gesendet und in der umgekehrten Richtung Aktionen auf die Lancope übertragen werden. Die besseren Möglichkeiten zur Analyse bietet die Lancope nicht nur in der Nachbereitung eines IT-Sicherheitsvoralls, sondern auch in der Erkennung einer möglichen Vorbereitung neuer Angriffe auf die IT-Infrastruktur des Forschungszentrums.

Insgesamt ist das ausgewählte System durch Eigenentwicklungen mit vertretbarem Aufwand, z.B. im Rahmen von Bachelor- und Masterarbeiten, flexibel anpassbar an die entstehenden Anforderungen im JuNet.

7. Literaturhinweise

[CYBERCRIME]	CYBERCRIME – Bundeslagebild 2011, Bundeskriminalamt,Wiesbaden, http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2011,templateId=raw,property=publicationFile.pdf/cybercrime2011.pdf
[JSC-RI-2-2012]	Richtlinie Nr. 2/2012 - IT-Sicherheitsrichtlinie des Forschungszentrums Jülich, http://intranet.fz-juelich.de/SharedDocs/Interne_Regelungen/IT-Sicherheitsrichtlinie_des_Forschungszentrums_Juelich_RL_2_2012_IR_119-1.pdf.pdf?__blob=publicationFile
[BSI-IDS-Leitfaden]	BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, https://www.bsi.bund.de/cln_165/ContentBSI/Publikationen/Studien/ids02/index_htm.html
[BSI-IDS-Grundlagen]	Grundlagen zu Intrusion-Detection-Systemen, https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/ids02/gr_index_htm.html;jsessionid=9AE086B3ADF1735BC2C4E73E90D94924.2_cid251
[PONEMON]	Sourcefire-Auftragsstudie belegt Bedarf an Intrusion Detection in Firewalls der nächsten Generation., http://www.tomsnetworking.de/aktuelles/news_beitrag/news/4615/index.html
[PENTEST]	Bericht zum Penetrationstest der Applikationen www.fz-juelich.de, www.deep-project.eu und www.hrecruiting.de, T-Systems, Aug.2012
[ERNST-YOUNG2012]	Fighting to close the gap – Ernst & Young 2012 Global Information Security Survey, http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf
[KPMG-IT-Sec-Survey]	Luxembourg IT Security Survey 2012-2013 kpmg-lu, http://www.google.de/url?sa=t&rct=j&q=information%20security%20survey%202012&source=web&cd=8&cad=rja&ved=0CHYQFjAH&url=http%3A%2F%2Fwww.kpmg.com%2FLU%2Fen%2FIssuesAndInsights%2FArticlespublications%2FDocuments%2FLux-IT-Security-Survey-2012-2013.pdf&ei=JTb9UM2vKYHPtAbL0oGYAw&usg=AFQjCNEIG-ZEiiydMgMrdeay7nURJL1SzQ&bvm=bv.41248874,d.Yms
[Incident-Cost-Analysis]	Developing an Effective Incident Cost Analysis Mechanism, Symantec, http://www.symantec.com/connect/articles/developing-effective-incident-cost-analysis-mechanism
[ITU-Financial-Study]	ITU Study on the Financial Aspects of Network Security: Malware and Spam, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf


JÜLICH
FORSCHUNGSZENTRUM